10.11.2004

#2

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

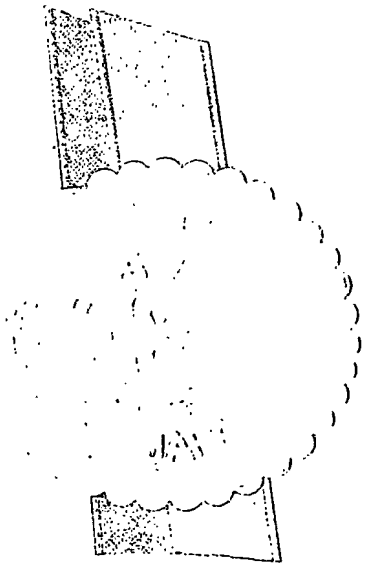
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１１月２１日

出願番号
Application Number: 特願２００３－３９２３７７

[ST. 10/C]: [ＪＰ２００３－３９２３７７]

出願人
Applicant(s): キヤノン株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

２００４年１２月１７日

特許庁長官
Commissioner,
Japan Patent Office 小川洋

出証番号　出証特２００４－３１１５６９７

【書類名】　特許願
【整理番号】　256838
【提出日】　平成15年11月21日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 12/14　320
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
　【氏名】　鈴木　勝也
【特許出願人】
　【識別番号】　000001007
　【氏名又は名称】　キヤノン株式会社
　【代表者】　御手洗　冨士夫
【代理人】
　【識別番号】　100081880
　【弁理士】
　【氏名又は名称】　渡部　敏彦
　【電話番号】　03(3580)8464
【手数料の表示】
　【予納台帳番号】　007065
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9703713

【書類名】特許請求の範囲
【請求項１】
非接触ＩＣに記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムであって、
前記機密エリアに対する前記非接触ＩＣの持出し／持込み状況を検知する検知手段と、
前記検知手段により、前記機密エリアからの前記非接触ＩＣの持出しが検知された場合に、当該非接触ＩＣに記録された機密データに対して所定の漏洩防止処理を施す漏洩防止手段と、
を有することを特徴とするセキュリティシステム。
【請求項２】
前記漏洩防止手段は、前記非接触ＩＣに記録された機密データを所定の装置に退避した後に、該非接触ＩＣに記録された退避に係る機密データを消去することを特徴とする請求項１に記載のセキュリティシステム。
【請求項３】
前記漏洩防止手段は、前記非接触ＩＣが機密エリアの中に持込まれる場合に、前記サーバ装置に退避した機密データを該非接触ＩＣに書き戻す書戻手段を有することを特徴とする請求項２に記載のセキュリティシステム。
【請求項４】
前記漏洩防止手段は、前記非接触ＩＣに記録された機密データをアクセス不可状態にすることを特徴とする請求項１に記載のセキュリティシステム。
【請求項５】
非接触ＩＣに記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を含むセキュリティシステムであって、
前記リーダ／ライタは、前記ゲート手段によって形成されるセキュリティエリアの外に前記非接触ＩＤが持出される場合に、該非接触ＩＣに記録された機密データに対して前記リーダ／ライタを用いて所定の漏洩防止処理を施す制御手段を有することを特徴とするセキュリティシステム。
【請求項６】
前記制御手段は、前記非接触ＩＣに記録された機密データを読み取って所定の装置に退避した後に、該非接触ＩＣに記録された退避に係る機密データを消去することを特徴とする請求項５に記載のセキュリティシステム。
【請求項７】
前記制御手段は、前記非接触ＩＣが前記セキュリティエリアの中に持込まれる場合に、前記所定の装置に退避した機密データを該非接触ＩＣに書き戻す書戻手段を有することを特徴とする請求項６に記載のセキュリティシステム。
【請求項８】
前記制御手段は、前記非接触ＩＣに記録された機密データをアクセス不可状態にすることを特徴とする請求項５に記載のセキュリティシステム。
【請求項９】
非接触ＩＣに記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムの制御方法であって、
前記機密エリアに対する前記非接触ＩＣの持出し／持込み状況を検知する検知工程と、
前記検知工程により、前記機密エリアからの前記非接触ＩＣの持出しが検知された場合に、当該非接触ＩＣに記録された機密データに対して所定の漏洩防止処理を施す漏洩防止工程と、
を有することを特徴とするセキュリティシステムの制御方法。
【請求項１０】
非接触ＩＣに記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を含むセキュリティシステムの制御方法であって、
前記リーダ／ライタは、前記ゲート手段によって形成されるセキュリティエリアの外に

前記非接触ＩＤが持出される場合に、該非接触ＩＣに記録された機密データに対して前記リーダ／ライタを用いて所定の漏洩防止処理を施す制御工程を有することを特徴とするセキュリティシステムの制御方法。

【請求項１１】

非接触ＩＣに記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムにおける該非接触ＩＣ用のプログラムであって、

前記機密エリアに対する前記非接触ＩＣの持出し／持込み状況を検知する検知処理と、該検知処理により、前記機密エリアからの前記非接触ＩＣの持出しが検知された場合に、当該非接触ＩＣに記録された機密データに対する所定の漏洩防止処理とを行う内容を有することを特徴とするプログラム。

【請求項１２】

非接触ＩＣに記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を含むセキュリティシステムにおける該リーダ／ライタ用のプログラムであって、

前記ゲート手段によって形成されるセキュリティエリアの外に前記非接触ＩＤが持出される場合に、該非接触ＩＣに記録された機密データに対して所定の漏洩防止処理を施す内容を有することを特徴とするプログラム。

【請求項１３】

非接触ＩＣに記録された情報を非接触にてアクセスするリーダ／ライタを備えたゲート手段を有するセキュリティシステムにおける該非接触ＩＣ用のプログラムであって、

前記ゲート手段によって形成されるセキュリティエリアの外に前記非接触ＩＤが持出される場合に、前記リーダ／ライタからの指示に応じて、該非接触ＩＣに記録された機密データに対して所定の漏洩防止処理を施す内容を有することを特徴とするプログラム。

【書類名】明細書
【発明の名称】セキュリティシステム
【技術分野】
【０００１】
本発明は、ＲＦＩＤ（Ｒａｄｉｏ　Ｆｒｅｑｕｅｎｃｙ－　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ）タグのような非接触ＩＣに格納された機密データを保護する技術に関する。
【背景技術】
【０００２】
従来、磁気カード等の可搬性のある記憶媒体等を用いて入退出管理を行うセキュリティシステムが実現されている（例えば、特許文献１参照）。
【特許文献１】特開平１１－３０３４７８号公報
【発明の開示】
【発明が解決しようとする課題】
【０００３】
ところで、ＲＦＩＤタグのような非接触ＩＣの利用形態として、例えば、非接触ＩＣ内のメモリにＭＦＰ（複合機）に対するジョブ情報を格納し、このジョブ情報を非接触でＭＦＰにダウンロードして実行させることが考えられる。
【０００４】
このような利用形態において、非接触ＩＣのメモリに社外秘、或いは部門外秘等の機密データ（ジョブ情報、コマンドを含む）を格納した状態で、この非接触ＩＣを社外、或いは部門外等に持ち出した際に紛失してしまったような場合に、非接触ＩＣ内のメモリに格納された機密データが第３者により読み出されてしまい、機密状態を維持できなくなって、機密データのセキュリティが低下する可能性がある。
【０００５】
そこで、本発明は、非接触ＩＣに格納された機密データが所定エリア外で第３者に漏洩するのを防止し得るセキュリティシステム、その制御方法、及びプログラムを提供することを目的とする。
【課題を解決するための手段】
【０００６】
上記目的を達成するため、本発明は、非接触ＩＣに記録された機密データが機密エリアの外部で漏洩するのを防止するセキュリティシステムであって、前記機密エリアに対する前記非接触ＩＣの持出し／持込み状況を検知する検知手段と、前記検知手段により、前記機密エリアからの前記非接触ＩＣの持出しが検知された場合に、当該非接触ＩＣに記録された機密データに対して所定の漏洩防止処理を施す漏洩防止手段とを有している。
【発明の効果】
【０００７】
本発明によれば、非接触ＩＣに格納された機密データが所定エリア外で第３者に漏洩するのを防止し得るセキュリティシステム、その制御方法、及びプログラムを提供することが可能となり、第３者による機密データの悪用を回避することが可能となる。
【発明を実施するための最良の形態】
【０００８】
以下、本発明を実施するための最良の形態を、図面に基づいて詳細に説明する。
【０００９】
図１は、本発明に係るセキュリティシステムのシステム構成図である。本システムにおいては、門、ドア等の物理的な複数のゲートや物理的な壁（不図示）等によって外界から区分されたセキュリティエリア（機密エリアとも言う）１００を想定しており、このセキュリティエリア１００内には、セキュリティサーバ１０３、ＭＦＰ（複合機）１０５、文書サーバ１０６、清算装置１０８が配備されている。なお、門、ドア等の物理的な複数ゲートには、これらゲートを開閉制御するゲート制御部１０１が設けられている。
【００１０】

また、複数のゲートには、ＲＦＩＤタグ（非接触ＩＣ）１０４内の不揮発性メモリ２０１（図２参照）にアクセスするためのリーダ／ライタ１０９も設置されている。また、各ゲートに設置された各リーダ／ライタ１０９は、第１のネットワーク１０２によって相互に接続されており、この第１のネットワーク１０２には、ゲート制御部１０１、セキュリティサーバ１０３も接続されている。

【００１１】

このようなネットワーク構成の下で、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１に格納されたユーザＩＤ４０１（図４参照）をリーダ／ライタ１０９で読み出してセキュリティサーバ１０３に転送し、このセキュリティサーバ１０３にて当該ユーザの入退出を管理すると共に、ゲート制御部１０１を介してゲートを開閉することにより、セキュリティエリア１００を形成している。

【００１２】

なお、本実施形態では、セキュリティサーバ１０３によるユーザの入退出管理に応じて、物理的なゲートをゲート制御部１０１により開閉制御しているが、必ずしも物理的なゲートをゲート制御部１０１により開閉制御する必要はない。

【００１３】

また、後で詳細に説明するように、機密データ（ジョブ情報、コマンドを含む）が格納されＲＦＩＤタグ１０４をセキュリティエリア１００の外に持ち出す場合は、ＲＦＩＤタグ１０４内の機密データをリーダ／ライタ１０９で読み出してセキュリティサーバ１０３に退避すると共に、ＲＦＩＤタグ１０４内の機密データを消去することにより、セキュリティエリア１００外で機密データが第３者に漏洩するのを防止している。

【００１４】

また、ＲＦＩＤタグ１０４をセキュリティエリア１００の中に再度持ち込む場合に、セキュリティサーバ１０３に退避した機密データをリーダ／ライタ１０９を介してＲＦＩＤタグ１０４に書き戻すことにより、セキュリティエリア１００内で機密データを自由に利用できるようにしている。

【００１５】

セキュリティエリア１００内のＭＦＰ（複合機）１０５、清算装置１０８には、それぞれ、リーダ／ライタ１０５ａ、１０８ａが搭載されており、後述するように、セキュリティエリア１００内では、ＭＦＰ（複合機）１０５、清算装置１０８は、それぞれリーダ／ライタ１０５ａ、１０８ａを介して、ＲＦＩＤタグ１０４内のメモリに対して自由にアクセスできるように構成されている。

【００１６】

なお、第１のネットワーク１０２は、機密性を向上させるため、外界のネットワーク（インターネット等）とは物理的に分離されていることが望ましいが、物理的に分離することなく、ゲートウェイ等により情報的に分離するようにしてもよい。

【００１７】

ＭＦＰ１０５と文書サーバ１０６は、第２のネットワーク１０７を介して接続されている。この第２のネットワーク１０７は、ＬＡＮ、ＳＡＮ（Ｓｔｏｒａｇｅ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）等により構成されているが、必ずしも第１のネットワーク１０２と物理的に接続されている必要はない。

【００１８】

ＭＦＰ１０５に対するＲＦＩＤタグ１０４の利用形態としては、ＭＦＰ１０５に搭載されたリーダ／ライタ１０５ａにＲＦＩＤタグ１０４をかざすことで、このＲＦＩＤタグ１０４に格納されたＦＡＸ送信先情報、電子メールアドレス、文書サーバ１０６に格納された文書データの位置情報等を非接触にてＭＦＰ１０５にダウンロードし、それぞれＦＡＸ送信、電子メール送信、文書印刷出力を実行させること等が可能である。また、ＭＦＰ１０５に搭載されたリーダ／ライタ１０５ａにＲＦＩＤタグ１０４を近づけた状態で、ＭＦＰ１０５の操作部（不図示）からＦＡＸ送信先情報、メールアドレス、文書サーバ１０６に格納された文書データの位置情報等を入力し、リーダ／ライタ１０５ａを介して非接触

にてＲＦＩＤタグ１０４に格納することも可能である。

【００１９】

清算装置１０８は、例えば食堂等に設置されており、この清算装置１０８に対するＲＦＩＤタグ１０４の利用形態としては、例えば清算装置１０８がＲＦＩＤタグ１０４に格納されたユーザＩＤ等に基づいて清算処理を行うことが可能である。この際、清算処理としては、予めプリペイドカード方式で入金を行っておくことで、ＲＦＩＤタグ１０４に格納された残高情報を元に清算する方式でも、或いは清算装置１０８に接続された清算用サーバ（不図示）によって、ユーザ毎の代金情報を上記清算サーバ内に積算・記憶し、１ヶ月等の間隔で清算を行うような構成でもよい。また、毎回の食事の内容等を上記清算サーバ又はＲＦＩＤタグ１０４に格納し、後から履歴を参照できる構成にしてもよい。

【００２０】

上記ＭＦＰ１０５及び、清算装置１０８に対するＲＦＩＤタグ１０４の利用形態は、あくまでも一例であり、且つ本発明とは直接関係が無いため、詳細な説明は省略する。なお、ＲＦＩＤタグ１０４は、上記ＭＦＰ１０５、清算装置１０８以外のセキュリティエリア１００内の各種の電子情報機器で利用することができる。

【００２１】

［ＲＦＩＤタグ］

図２は、ＲＦＩＤタグ１０４の構成を示すブロック図である。ＲＦＩＤタグ１０４は、非接触ＩＣチップ、或いはデータキャリアとも呼ばれ、リーダ／ライタと無線で（すなわち非接触で）交信することが可能となっている。本実施形態では、カード型のＲＦＩＤタグを想定しており、このカード型ＲＦＩＤタグ内には、以下のデバイスを内蔵した非接触ＩＣチップが内包されている。

【００２２】

すなわち、ＲＦＩＤタグ（非接触ＩＣチップ）１０４には、不揮発性メモリ２０１、電波を送受信するためのアンテナ部２０２、共振コンデンサ部２０３、電流の整流・平滑を行うための電力生成部２０４、電波の復調・変調を行うための復変調回路２０５、及び制御部２０６が形成されている。このＲＦＩＤタグ１０４は、バッテリ等の電源を内蔵しておらず、リーダ／ライタから供給される電波に基づいて電力を誘電している。

【００２３】

すなわち、アンテナ部２０２は、共振コンデンサ部２０３との組み合わせで共振回路を形成している。一方、リーダ／ライタは、後述するように、常時、電力生成用の電波（交流磁界）を発している。このリーダ／ライタにＲＦＩＤタグ１０４をかざすと、ＲＦＩＤタグ１０４内の上記共振回路には電磁誘導作用により誘導電流が発生する。この誘導電流は、電力生成部２０４に出力され、電力生成部２０４は、入力された誘導電流を整流・平滑して所定電圧の電力を生成し、不揮発性メモリ２０１、制御部２０６、復変調回路２０５に供給する。制御部２０６は、ＲＦＩＤタグ１０４を全体的に制御するものである。

【００２４】

リーダ／ライタは、電力生成用の電波信号の他に各種のデータに係る電波信号も同時に送信しており、このデータに係る電波信号は、復変調回路２０５によって復調され、制御部２０６の制御の下に不揮発性メモリ２０１に書き込まれる。また、制御部２０６は、不揮発性メモリ２０１からデータを読み出し、復変調回路２０５によって変調してアンテナ部２０２を介して電波信号として送信する。

【００２５】

なお、制御部２０６は、ＲＯＭ（図示省略）を内蔵しており、このＲＯＭには、図５のフローチャートにおけるステップＳ５０２，Ｓ５０５～Ｓ５１０、図６のフローチャートにおけるステップＳ６０２，Ｓ６０６に対応するアプリケーションプログラムが格納されている。ただし、このアプリケーションプログラムは、不揮発性メモリ２０１に格納してもよい。

【００２６】

［リーダ／ライタ］

図３は、リーダ／ライタ１０９、１０５ａ、１０８ａの構成を示すブロック図である。リーダ／ライタ１０９、１０５ａ、１０８ａは、電波信号を送信するための送信アンテナ部３０１と、送信アンテナ部３０１から送信するデータ信号を変調する変調回路３０２と、電波信号を受信する受信アンテナ部３０３、受信アンテナ部３０３より受信した電波信号を復調する復調回路３０４、上位機器（本実施形態では、セキュリティサーバ１０３）との通信を行うＩ／Ｆ部３０６、及び制御部３０５を有しており、制御部３０５は、上記送信アンテナ部３０１、変調回路３０２、受信アンテナ部３０３、復調回路３０４、及びＩ／Ｆ部３０６を制御している。なお、送信アンテナ部３０１には、前述の電力生成用の電波を発するための交流電源３０７が接続されている。

【００２７】

制御部３０５は、セキュリティサーバ１０３からの指示により、変調回路３０２を用いて電力を供給するための電波、及び送信するデータを変調して、送信アンテナ部３０１を介して電波を発信させる。また、制御部３０５は、受信アンテナ部３０３で受信した電波信号を、復調回路３０４により復調させた後、データ信号として扱えるように変換することができる。

【００２８】

なお、制御部３０５は、ＲＯＭ（図示省略）を内蔵しており、このＲＯＭには、図５のフローチャートにおけるステップＳ５０２，Ｓ５０５～Ｓ５１０、図６のフローチャートにおけるステップＳ６０２，Ｓ６０６に対応するアプリケーションプログラムが格納されている。

【００２９】

［ＲＦＩＤタグの格納データ］

図４は、ＲＦＩＤタグ１０４の不揮発性メモリ２０１に格納されたデータを示す概念図である。

【００３０】

ＲＦＩＤタグ１０４内の不揮発性メモリ２０１には、当該ＲＦＩＤタグ１０４の所有権者のユーザＩＤ４０１と個別データ４０２が格納されている。このユーザＩＤ４０１としては、各ＲＦＩＤタグ１０４に対してそれぞれに固有の値（数値、記号等）が割り振られており、このユーザＩＤ４０１に基づいて当該ＲＦＩＤタグ１０４を所有するユーザを認証することができる。すなわち、各ＲＦＩＤタグ１０４内の不揮発性メモリ２０１に格納された各ユーザＩＤ４０１は、本システムの運用前に予めセキュリティサーバ１０３に登録されており、例えばゲートを通過する際に、リーダ／ライタ１０９によりＲＦＩＤタグ１０４からユーザＩＤ４０１を読み取り、セキュリティサーバ１０３に登録されたユーザＩＤ等と照合することで、当該ユーザがゲートを通過しても良いか否かを判断し（これを認証と呼ぶ）、入場／退出した旨がセキュリティサーバ１０３に記録される。

【００３１】

個別データ４０２は、１つのＲＦＩＤタグ１０４内に１つ又は複数の個別データ２０２が格納されている。各個別データ４０２は、それぞれ個別データＩＤ４０３、データ本体４０４、機密フラグ４０５によって構成されている。

【００３２】

個別データＩＤ４０３は、各個別データ４０２（すなわち、データ本体４０４）を識別するためのＩＤであり、電力生成用の電波信号個別データ４０２毎に固有の値（数値、記号等）が割り振られており、ユーザＩＤ４０１と組み合わせることで、ＭＦＰ１０５や清算装置１０８に対して、データ本体４０４の各種データを授受することができる。

【００３３】

データ本体４０４は、実際に読み書きされて各種処理に用いられる個別データ４０２の実体をなすデータであり、前述のように、ＭＦＰ１０５に関するデータとしては、ＦＡＸ送信先情報、電子メールアドレス、文書サーバ１０６に格納された文書データの位置情報等が読み書きされ。なお、ＭＦＰ１０５操作部から入力された情報を追加、或いは上書きすることも可能である。

【００３４】
また、清算装置１０８に関するデータとしては、予め入金された金銭データや、食事の履歴情報が読み書きされる。なお、金銭データは清算装置１０８に接続された清算サーバ（不図示）によってのみ書き換えられる情報である。食事の履歴情報は、清算装置１０８によって書き換えられる情報である。

【００３５】
機密フラグ４０５は、個別データ４０２毎に設定される情報であり、当該個別データ４０２が機密情報を含むのか否かを表している。本実施形態では、機密フラグ４０５がＯＮ（１）の場合は機密情報を含み、ＯＦＦ（０）の場合は機密情報を含まないものと定義している。この機密フラグ４０５は、セキュリティサーバ１０３に接続されるリーダ／ライタ１０９でのみ書き込みが可能となっている。

【００３６】
なお、本明細書では、機密フラグ４０５がＯＮとなっている個別データ４０２については、その個別データ４０２の全部が機密事項ではなく一部だけが機密事項となっている場合も、当該個別データ４０２全体を機密データと呼んでいる（特許請求の範囲も同趣旨）。

【００３７】
[退出処理]
次に、セキュリティエリア１００の中から外部に退出する場合の処理を、図５のフローチャートに基づいて説明する。

【００３８】
ユーザが、セキュリティエリア１００内から外部に退出する際に、ゲートに設置されたリーダ／ライタ１０９にＲＦＩＤタグ１０４をかざす（ステップＳ５０１）。すると、ＲＦＩＤタグ１０４には、リーダ／ライタ１０９から発せられた電波により電力が誘電され、リーダ／ライタ１０９との交信が可能となる。そこで、リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１から、ユーザＩＤ４０１を読み出してセキュリティサーバ１０３に送信する。（ステップＳ５０２）。

【００３９】
セキュリティサーバ１０３は、リーダ／ライタ１０９から受信したユーザＩＤ４０１が、当該セキュリティサーバ１０３に登録されており、かつ、そのユーザＩＤ４０１に係るユーザの入退出の状況が「入場」となっているか否かを判別することにより、当該ユーザの退出を認証するか否かを判別する（ステップＳ５０３）。

【００４０】
セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録されていない、或いは登録されていても当該ユーザＩＤ４０１に係るユーザの入退出の状況が「退出」となっている場合（この場合は、過去に不正にセキュリティエリア１００内に入場したことを意味する）は、当該ユーザの退出を認証せずに、所定の警告処理を行って（ステップＳ５０４）、終了する。この警告処理としては、例えば、ゲートに設置された表示装置（図示省略）に警告メッセージを表示する、ゲートに設置されたスピーカ（図示省略）により警告音を鳴らす、或いはゲート制御部１０１によりゲートを一時的に閉鎖状態にロックさせること等が考えられる。

【００４１】
一方、セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録され、かつ当該ユーザＩＤ４０１に係るユーザの入退出の状況が「入場」となっている場合は、当該ユーザの退出を認証し、当該ユーザＩＤ４０１に係るユーザの入退出の状況を「退出」に変更し、当該ユーザの退出を認証した旨の情報をリーダ／ライタ１０９に通知する（ステップＳ５０５）。

【００４２】
なお、本実施形態では、セキュリティサーバ１０３のメモリ容量を削減するため、セキ

ユリティサーバ１０３は、最新の入退出状況だけを記憶しているが、過去の全て、或いは複数の入退出状況（履歴）を記憶するようにしてもよい。

【００４３】

リーダ／ライタ１０９の制御部３０５は、当該ユーザの退出を認証した旨の情報を受信すると、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１から、１つの個別データ４０２に係る個別データＩＤ４０３と機密フラグ４０５を読み出して（ステップＳ５０６）、機密フラグ４０５がＯＮとなっているか否かを判別する（ステップＳ５０７）。

【００４４】

その結果、機密フラグ４０５がＯＮとなっていれば、リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、対応する個別データ４０２（データ本体４０４）をＲＦＩＤタグ１０４内の不揮発性メモリ２０１から読み出して、セキュリティサーバ１０３に退避させ（ステップＳ５０８）、不揮発性メモリ２０１上の当該個別データ４０２を消去して（ステップＳ５０９）、ステップＳ５１０に進む。一方、機密フラグ４０５がＯＦＦとなっていれば、リーダ／ライタ１０９の制御部３０５は、ステップＳ５０８の退避処理、ステップＳ５０９の消去処理を行うことなく、ステップＳ５１０に進む。

【００４５】

ステップＳ５１０では、リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１を参照し、機密フラグ４０５のチェック等を行っていない次の個別データ４０２が存在するか否かを判別する。その結果、機密フラグ４０５のチェック等を行っていない次の個別データ４０２が存在すれば、リーダ／ライタ１０９の制御部３０５は、ステップＳ５０６に戻り、当該次の個別データ４０２に対して同様の処理を行う。

【００４６】

一方、全ての個別データ４０２に対する機密フラグ４０５のチェック等の処理が完了した場合は、リーダ／ライタ１０９の制御部３０５は、例えばゲート制御部１０１によりゲートをオープンさせる等の入場処理を行い（ステップＳ５１１）、本処理を終了する。

【００４７】

［入場処理］

次に、セキュリティエリア１００の中から外部に退出する場合の処理を、図５のフローチャートに基づいて説明する。

【００４８】

ユーザは、セキュリティエリア１００の外から内部に入場する際に、ゲートに設置されたリーダ／ライタ１０９にＲＦＩＤタグ１０４をかざす（ステップＳ６０１）。すると、ＲＦＩＤタグ１０４には、リーダ／ライタ１０９から発せられた電波により電力が誘電され、リーダ／ライタ１０９との交信が可能となる。そこで、リーダ／ライタ１０９の制御部３０５は、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１から、ユーザＩＤ４０１を読み出してセキュリティサーバ１０３に送信する。（ステップＳ６０２）。

【００４９】

セキュリティサーバ１０３は、リーダ／ライタ１０９から受信したユーザＩＤ４０１が、当該セキュリティサーバ１０３に登録されており、かつ、そのユーザＩＤ４０１に係るユーザの入退出の状況が「退出」となっているか否かを判別することにより、当該ユーザの入場を認証するか否かを判別する（ステップＳ６０３）。

【００５０】

セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録されていない、或いは登録されていても当該ユーザＩＤ４０１に係るユーザの入退出の状況が「入場」となっている場合（この場合は、過去に不正にセキュリティエリア１００の外に退出したことを意味する）は、当該ユーザの入場を認証せずに、所定の

警告処理を行って（ステップＳ６０４）、終了する。この警告処理としては、例えば、ゲートに設置された表示装置に警告メッセージを表示する、ゲートに設置されたスピーカにより警告音を鳴らす、或いはゲート制御部１０１によりゲートを一時的に閉鎖状態にロックさせること等が考えられる。

【００５１】

一方、セキュリティサーバ１０３は、受信に係るユーザＩＤ４０１が当該セキュリティサーバ１０３に登録され、かつ当該ユーザＩＤ４０１に係るユーザの入退出の状況が「退出」となっている場合は、当該ユーザの入場を認証し、当該ユーザＩＤ４０１に係るユーザの入退出の状況を「入場」に変更し、当該ユーザの入場を認証した旨の情報をリーダ／ライタ１０９に通知する（ステップＳ６０５）。

【００５２】

リーダ／ライタ１０９の制御部３０５は、当該ユーザＩＤ４０１に係るユーザの入場を認証した旨の情報を受信すると、当該ユーザＩＤ４０１に係る退避された個別データ４０２をセキュリティサーバ１０３に照会して送信してもらい、ＲＦＩＤタグ１０４の制御部２０６と協働して、ＲＦＩＤタグ１０４内の不揮発性メモリ２０１に書き戻す（ステップＳ６０６）。

【００５３】

次に、リーダ／ライタ１０９の制御部３０５は、当該ユーザＩＤ４０１に係る退避された他の個別データ４０２が存在するか否かをセキュリティサーバ１０３に問合せ（ステップＳ６０７）、退避された他の個別データ４０２が存在する場合は、ステップＳ６０６に戻ることにより、当該他の個別データ４０２をＲＦＩＤタグ１０４内の不揮発性メモリ２０１に書き戻す。

【００５４】

なお、セキュリティサーバ１０３は、セキュリティサーバ１０３内のメモリ（図示省略）を有効利用するため、書き戻した個別データ４０２は消去している。また、セキュリティサーバ１０３は、上記のように、リーダ／ライタ１０９の制御部３０５からの照会や問合せに応答して、退避に係る個別データ４０２をリーダ／ライタ１０９に送信するのではなく、ステップＳ６０２でリーダ／ライタ１０９から受信したユーザＩＤ４０１に基づいて、能動的に退避に係る個別データ４０２を検索してリーダ／ライタ１０９に送信するようにしてもよい。

【００５５】

一方、退避された他の個別データ４０２が存在しない場合は、リーダ／ライタ１０９の制御部３０５は、例えばゲート制御部１０１によりゲートをオープンさせる等の入場処理を行い（ステップＳ６０８）、本処理を終了する。

【００５６】

このように、本実施形態では、セキュリティエリア１００の外にＲＦＩＤタグ１０４を持ち出す場合に、ＲＦＩＤタグ１０４から機密データを読み出してセキュリティサーバ１０３に退避した後に、ＲＦＩＤタグ１０４上の退避に係る機密データを消去し、セキュリティエリア１００の中にＲＦＩＤタグ１０４を持ち込む場合に、退避に係る機密データをＲＦＩＤタグ１０４に書き戻して復元しているので、機密データがセキュリティエリア１００の外で第３者に漏れて悪用されるのを回避することが可能となる。また、機密データの退避、消去、書戻し処理は、ＲＦＩＤタグ１０４をリーダ／ライタ１０９にかざした際に自動的に行われるので、ユーザの負担が増大することはない。

【００５７】

また、ＲＦＩＤタグ１０４にはバッテリを搭載する必要がないので、ＲＦＩＤタグ１０４の小型化が可能になると共に、セキュリティシステムを安価に構築することが可能となる。さらに、ユーザ認証を受けないと機密データの復元は行われないので、万一、ユーザ認証を受けずに不正にセキュリティエリア１００の中に入場したとしても、機密データを利用できなくなり、セキュリティ機能が更に向上する。

【００５８】

［実施形態の変形例］
上記のように、ＲＦＩＤタグ１０４に格納された機密データを退避、消去、書戻しを行うことなく、以下のようにして、機密データの漏洩を防止するようにしてもよい。

【００５９】
すなわち、個別データ４０２の構成データとして、読出可能フラグを定義し、セキュリティエリア１００の外にＲＦＩＤタグ１０４を持出す際には、機密データに係る読出可能フラグを読出不可状態に設定し、且つセキュリティエリア１００の中にＲＦＩＤタグ１０４を持ち込む際には、機密データに係る読出可能フラグを読出可能状態に設定することで、セキュリティエリア１００の外では、機密データの漏洩を防止すると共に、セキュリティエリア１００の中では、機密データを自由に利用できるようにしてもよい。

【００６０】
この場合、上記読出可能フラグは、上記セキュリティサーバ１０３によって当該ＲＦＩＤタグ１０４のユーザが認証された場合にのみ、例えばリーダ／ライタ１０９によりフラグ値を変更できるようにする必要がある。また、ＲＦＩＤタグ１０４においては、制御部２０６、又はメモリコントローラ（不図示）内に、上記読出可能フラグが読出不可状態に設定された個別データ（機密データ）を読出せないようにする制御機構を設け、ＲＦＩＤタグ用の市販のリーダ／ライタ等では、この機密データを読出せないようにする必要がある。

【００６１】
なお、上記実施形態例では、機密データの退避、消去、或いは書戻しの処理を行う必要があるため、入退出管理に要する時間が長くなる可能性が考えられる。一方、変形例では、機密データを直接処理することはないので、入退出管理に要する時間は短くなるが、機密データが形式上セキュリティエリア１００の外に持ち出されてしまい、セキュリティの点では多少の不安が残る。上記実施形態例と変形例の何れを選択するかは、セキュリティ性と入退出管理の所要時間との何れを重要視するかで決定すればよい。

【００６２】
なお、個別データ４０２の構成データとして、上記読出可能フラグの代わりに、アクセス可能フラグを定義することにより、機密データの上に他のデータが上書きされる等して機密データが破壊されるのを防止することも可能である。

【００６３】
また、上記のようにＲＦＩＤタグを入退出管理に利用せず、各種の装置で使用するデータを記録するだけの目的で利用する場合にも、本発明を適用することが可能である。この場合は、機密エリアに対するＲＦＩＤタグの持出し／持込みを検知する手段としては、ＲＦＩＤタグ用のリーダ／ライタを用いる必要はなく、例えば、パチンコ店、ゲームセンタ等の遊技場でＲＦＩＤタグを遊戯代金の清算媒体として利用するような場合において、所定の装置により遊技場に磁場（すなわち、機密エリア）を形成し、ＲＤＩＤタグには磁場を検知するデバイスを搭載し、このデバイスにより機密エリアに対するＲＦＩＤタグの持出し／持込みを検知することも可能である。

【００６４】
なお、上記の遊戯場でＲＦＩＤタグを遊戯代金の清算媒体として利用する例では、上記実施形態、又は変形例に係る機密データの漏洩防止処理は、ＲＦＩＤタグに格納されたプリペード情報が他の経営者に係る遊技場で使用されるのを回避するために行われる。

【００６５】
また、ＲＦＩＤタグにバッテリを搭載することも可能である。この場合は、ＲＦＩＤタグの制御部は、リーダ／ライタの制御部と協働することなく、主体的に上記実施形態、又は変形例に係る機密データの漏洩防止処理を実行するように構成することも可能である。

【００６６】
さらに、機密データの漏洩防止処理として、機密エリアの外にＲＦＩＤタグを持出す際に、当該ＲＦＩＤタグ内の機密データを暗号化し、機密エリアの中にＲＦＩＤタグを持込む際に（必要に応じてユーザ認証も行って）、当該ＲＦＩＤタグ内の暗号化された機密デ

ータを復号化することも可能である。

【００６７】

また、ＲＦＩＤタグの通信方式は、電波、又は電磁波を用いることなく、例えば、赤外線等の光を用いた通信方式でもよい。また、ＲＦＩＤタグの形状は、カード型でなく、ラベル型、コイン型、箱型、スティック型等であってもよい。

【００６８】

さらに、本発明の目的は、上記実施形態、変形例等の機能を実現するソフトウェアのプログラムコードをＲＦＩＤタグ、リーダ／ライタに無線通信等により非接触でダウンロードし、ＲＦＩＤタグ、リーダ／ライタの制御部がダウンロードに係るプログラムコードを実行することによっても、達成されることは言うまでもない。

【００６９】

この場合、上記プログラムコード自体が前述した実施形態、変形例等の機能を実現することになり、そのプログラムコードを記憶した記憶媒体は本発明を構成することになる。また、上記プログラムコードを実行することにより、前述した実施形態、変形例等の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、ＲＦＩＤタグ、リーダ／ライタ上で稼動しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態、変形例等の機能が実現される場合も含まれることは言うまでもない。

【図面の簡単な説明】

【００７０】

【図１】本発明を実施するための最良の形態に係るセキュリティシステムの概略構成を示すシステム構成図である。

【図２】上記セキュリティシステムのＲＦＩＤタグの概略構成を示すブロック図である。

【図３】上記セキュリティシステムのリーダ／ライタの概略構成を示すブロック図である。

【図４】上記ＲＦＩＤタグの不揮発性メモリ内のデータの構成を示す概念図である。

【図５】セキュリティエリアからＲＦＩＤタグを持ち出す場合のセキュリティシステムの処理を示すフローチャートである。

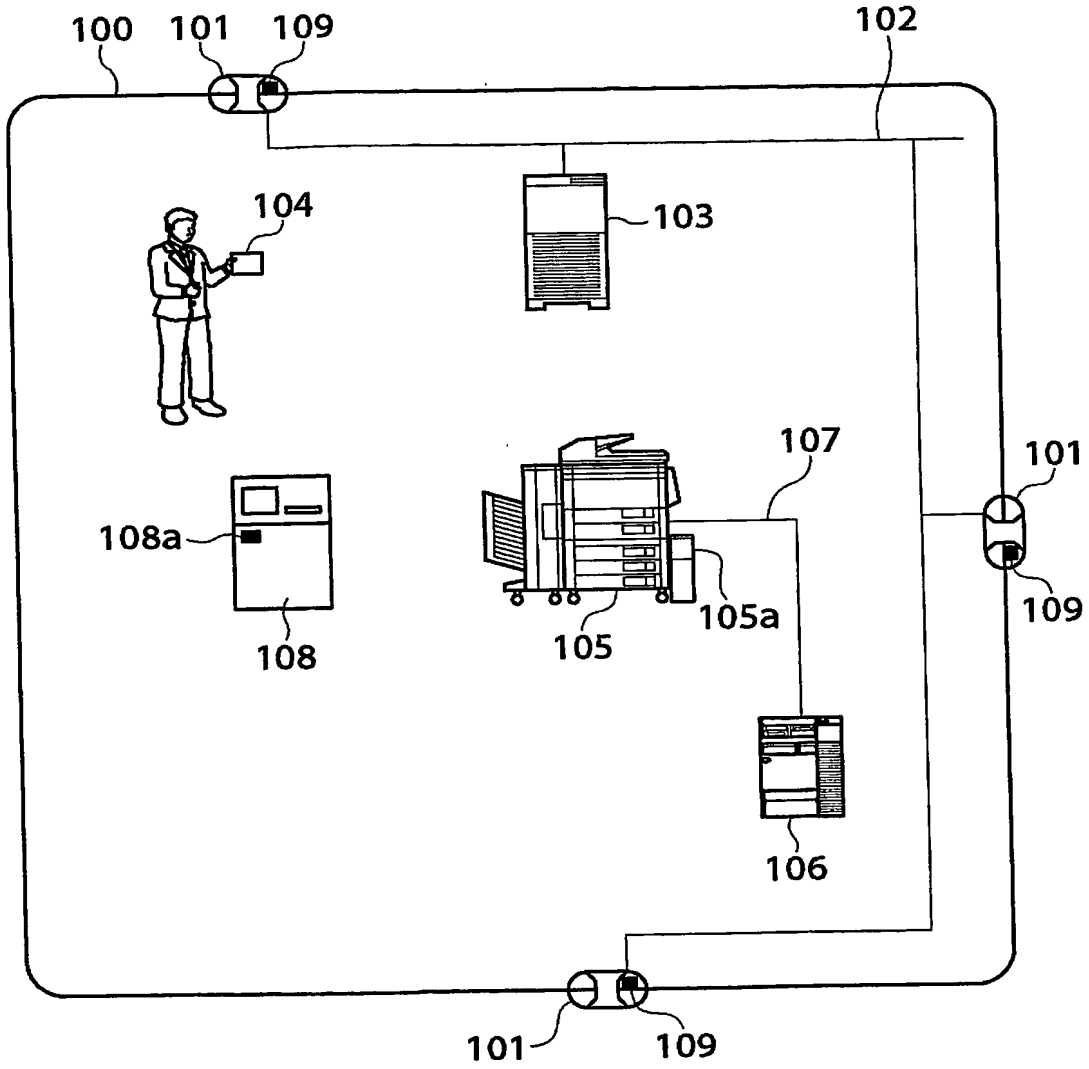
【図６】セキュリティエリアにＲＦＩＤタグを持ち込む場合のセキュリティシステムの処理を示すフローチャートである。

【符号の説明】

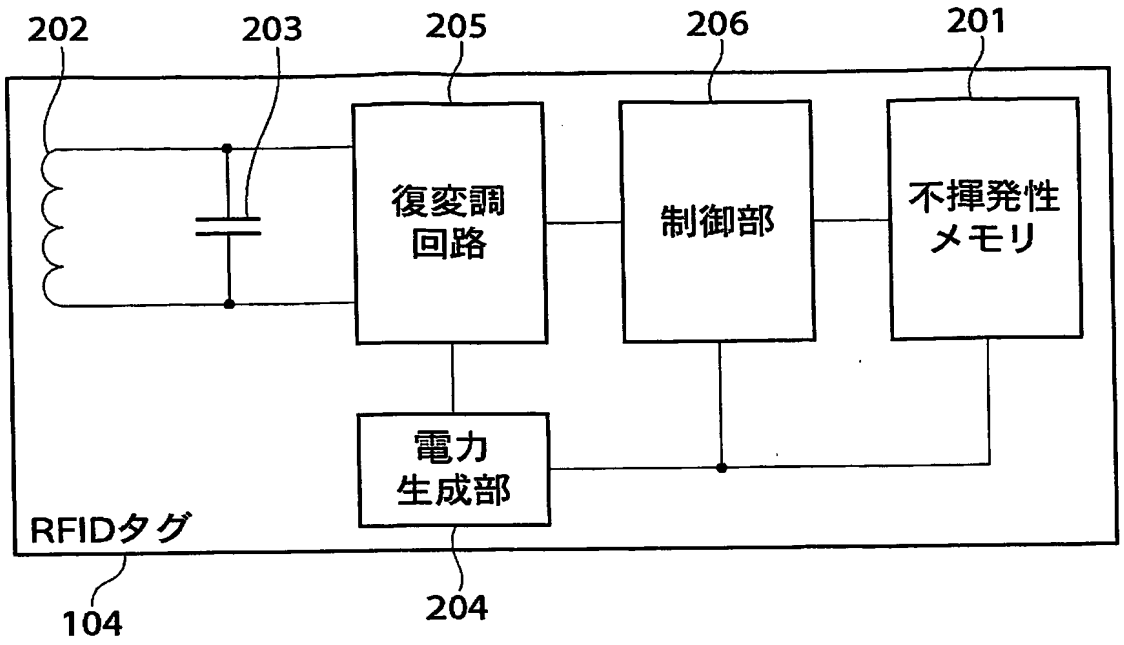
【００７１】

１００…セキュリティエリア
１０１…ゲート制御部
１０３…セキュリティサーバ
１０４…ＲＦＩＤタグ
１０９、１０５ａ，１０８ａ…リーダ／ライタ
２０１…不揮発性メモリ
２０５…ＲＦＩＤタグの制御部
３０５…リーダ／ライタの制御部
４０１…ユーザＩＤ
４０２…個別データ
４０５…機密フラグ

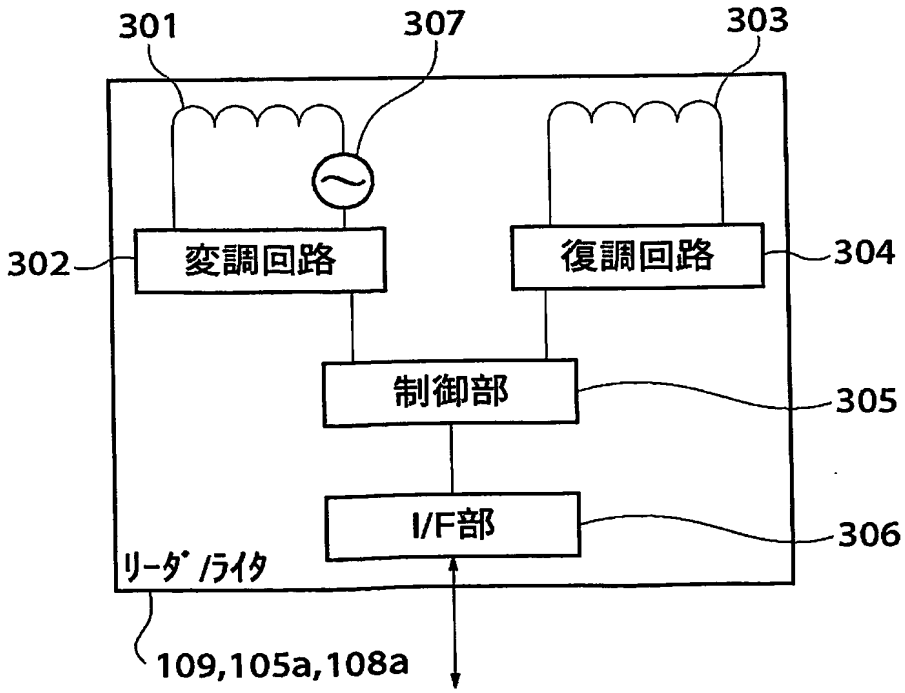
【書類名】図面
【図１】


100
101
109
102
104
103
107
101
108a
105a
109
108
105
106
101
109

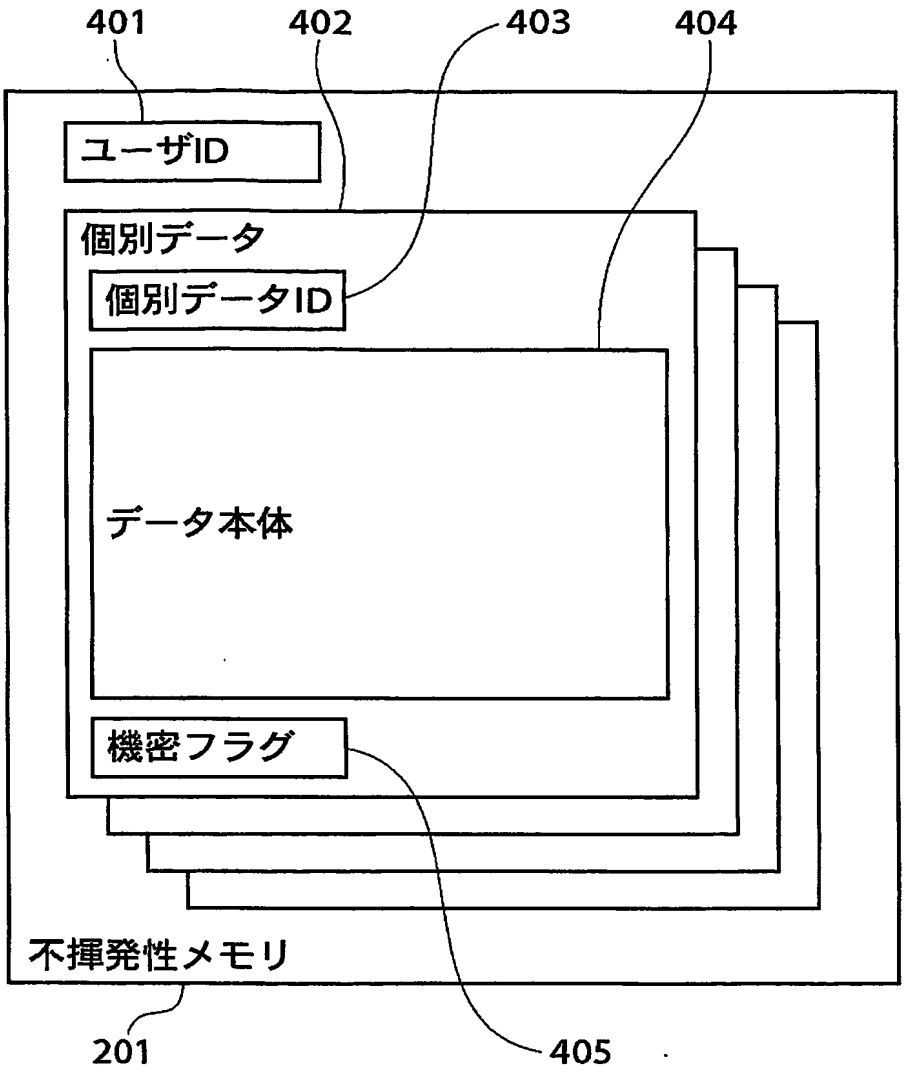
【図２】


202
203
205
206
201
復変調
回路
制御部
不揮発性
メモリ
電力
生成部
RFIDタグ
104
204

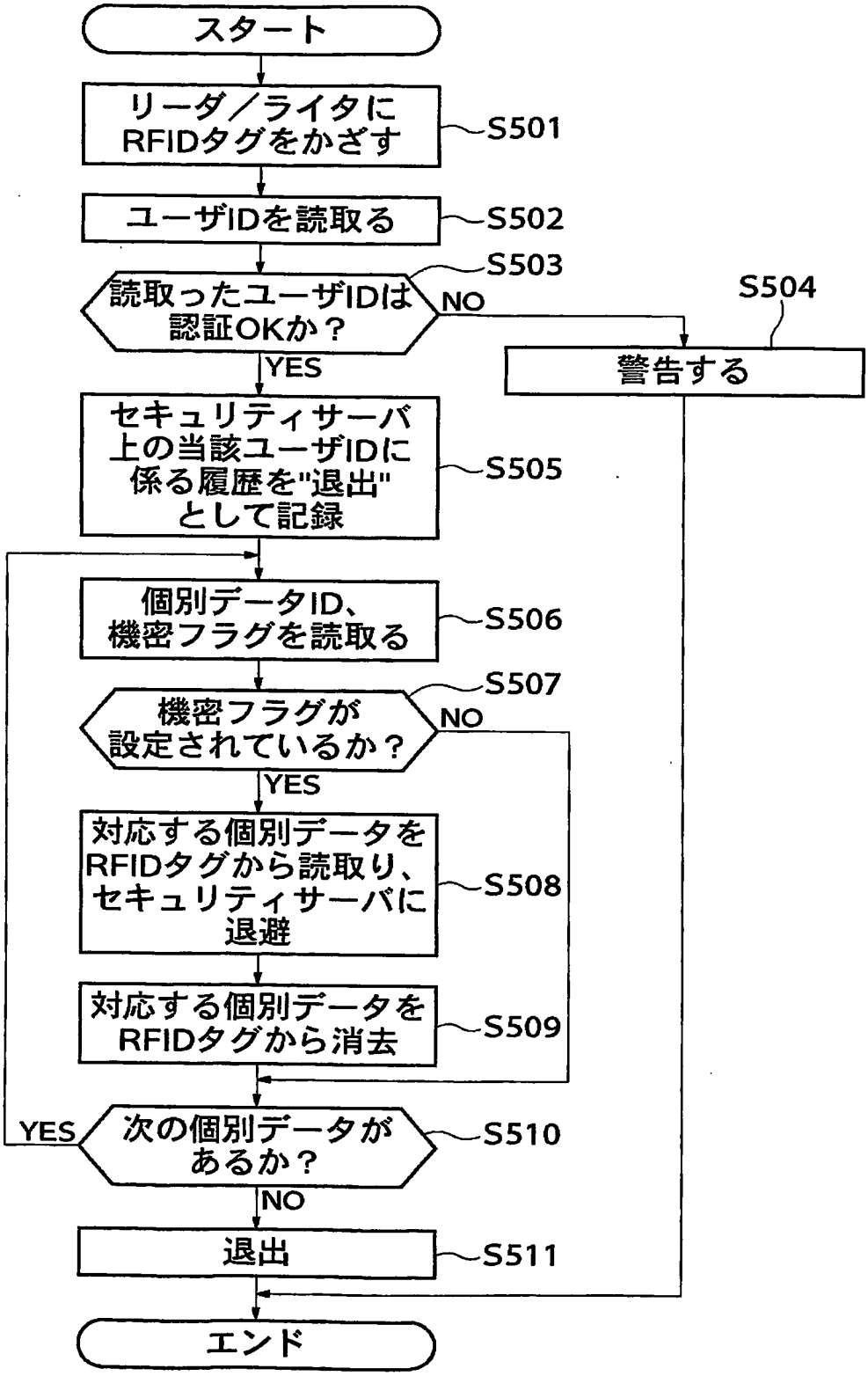
【図３】


301
307
303
302
変調回路
復調回路
304
制御部
305
I/F部
306
ﾘｰﾀﾞ/ﾗｲﾀ
109,105a,108a

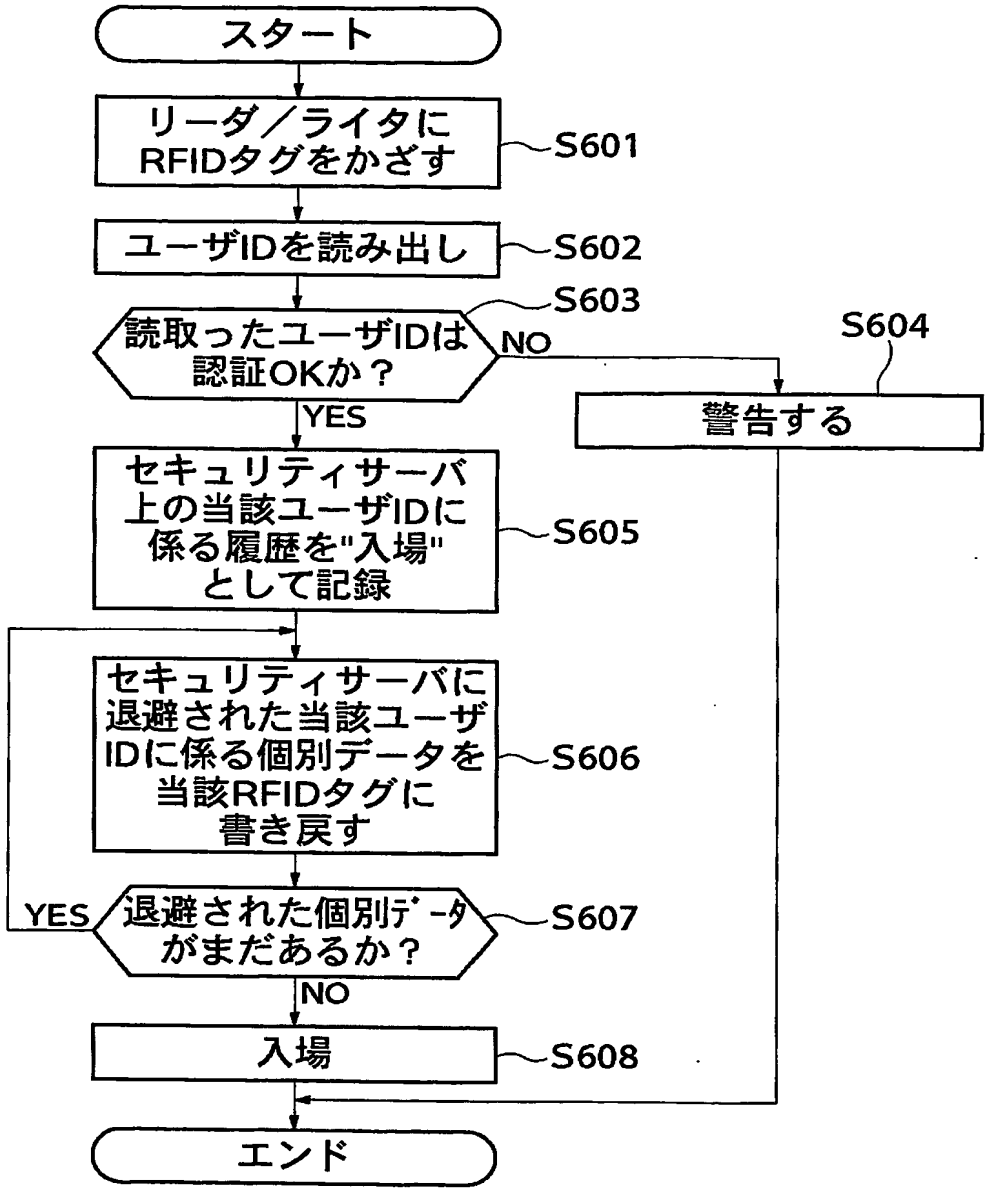
【図４】


401
402
403
404
ユーザID
個別データ
個別データID
データ本体
機密フラグ
不揮発性メモリ
201
405

【図５】


スタート
リーダ／ライタに
RFIDタグをかざす
S501
ユーザIDを読取る
S502
S503
読取ったユーザIDは
認証OKか？
NO
S504
警告する
YES
セキュリティサーバ
上の当該ユーザIDに
係る履歴を"退出"
として記録
S505
個別データID、
機密フラグを読取る
S506
S507
機密フラグが
設定されているか？
NO
YES
対応する個別データを
RFIDタグから読取り、
セキュリティサーバに
退避
S508
対応する個別データを
RFIDタグから消去
S509
YES
次の個別データが
あるか？
S510
NO
退出
S511
エンド

【図６】


スタート
リーダ／ライタにRFIDタグをかざす
S601
ユーザIDを読み出し
S602
S603
読取ったユーザIDは認証OKか？
NO
S604
警告する
YES
セキュリティサーバ上の当該ユーザIDに係る履歴を"入場"として記録
S605
セキュリティサーバに退避された当該ユーザIDに係る個別データを当該RFIDタグに書き戻す
S606
YES
退避された個別ﾃﾞｰﾀがまだあるか？
S607
NO
入場
S608
エンド

【書類名】要約書
【要約】
【課題】　非接触ＩＣに格納された機密データが所定エリア外で第３者に漏洩するのを防止できるようにする。
【解決手段】　セキュリティエリア１００の外にＲＦＩＤタグ１０４を持ち出す場合に、ＲＦＩＤタグ１０４から機密データを読み出してセキュリティサーバ１０３に退避した後に、ＲＦＩＤタグ１０４から退避に係る機密データを消去し、セキュリティエリア１００の中にＲＦＩＤタグ１０４を持ち込む場合に、ＲＦＩＤタグ１０４に退避に係る機密データを書き戻して復元する。
【選択図】　図１

特願２００３－３９２３７７

出　願　人　履　歴　情　報

識別番号　　[０００００１００７]

１．変更年月日　　１９９０年　８月３０日
　[変更理由]　　新規登録
　　住　所　　東京都大田区下丸子３丁目３０番２号
　　氏　名　　キヤノン株式会社